Nombre del Estudiante: Josué David Paucar Erazo

Nombre de la Materia: Lógica de Programación

Título del Trabajo: Diagrama Funcional y de Arquitectura

Nombre del Profesor: Monica Patricia Salazar Tapia

Carrera: Ingeniería en Ciberseguridad

Modalidad: Online

Identificación del Estudiante: 1722902713

Semestre: Primer Semestre 2024

Programa a desarrollar: Generador Seguro de Contraseñas

Resolución del Problema

1. Identificar el Problema

El problema a resolver es la necesidad de generar contraseñas seguras que sean difíciles de adivinar o descifrar. Esto es crucial para proteger las cuentas y la información sensible de los usuarios contra accesos no autorizados.

2. Comprender el Problema

Para comprender mejor el problema, consideremos los siguientes aspectos:

- **Requisitos de Seguridad:** Las contraseñas deben cumplir con ciertos criterios de seguridad, como longitud mínima, combinación de caracteres (letras mayúsculas y minúsculas, números, símbolos), y no ser predecibles.
- **Facilidad de Uso:** La aplicación debe ser fácil de usar, permitiendo a los usuarios especificar sus criterios y recibir una contraseña segura rápidamente.
- **Almacenamiento y Validación:** Las contraseñas generadas deben ser verificadas para asegurar que cumplen con los requisitos de seguridad establecidos.

3. Identificar Soluciones Alternativas

Podemos considerar varias formas de abordar este problema:

1. **Generador de Contraseñas Simple:** Utilizar un algoritmo básico que combine letras, números y símbolos para crear contraseñas al azar.
2. **Generador de Contraseñas Configurable:** Permitir a los usuarios especificar criterios personalizados, como longitud y tipos de caracteres.
3. **Generador de Contraseñas con Validación:** Incorporar un mecanismo de validación para verificar que la contraseña generada cumpla con los requisitos de seguridad.
4. **Generador de Contraseñas con Almacenamiento Seguro:** No solo generar y validar, sino también almacenar las contraseñas generadas de manera segura.

4. Seleccionar la Mejor Solución

La mejor solución será la que equilibre seguridad y facilidad de uso, y que cubra todos los requisitos necesarios. En este caso, optaré por una combinación de las soluciones 2 y 3:

- **Generador de Contraseñas Configurable con Validación:** Permitirá a los usuarios especificar criterios personalizados y asegurará que las contraseñas generadas cumplan con los estándares de seguridad.

5. Listar los Pasos de la Solución Seleccionada

1. **Diseño de la Interfaz de Usuario:** Crear una interfaz donde los usuarios pueden ingresar sus criterios (longitud de la contraseña, tipos de caracteres).
2. **Desarrollo del Algoritmo de Generación:** Implementar un algoritmo que genere contraseñas basadas en los criterios especificados.
3. **Desarrollo del Algoritmo de Validación:** Implementar un algoritmo que valide las contraseñas generadas asegurándose que cumpla con los requisitos de seguridad.
4. **Integración:** Integrar la interfaz de usuario con los algoritmos de generación y validación.
5. **Pruebas Unitarias:** Realizar pruebas unitarias para verificar que los componentes individuales funcionan correctamente.
6. **Pruebas de Integración:** Probar la aplicación en su totalidad para asegurar que la generación y validación de contraseñas funcionan según lo esperado.
7. **Implementación Final:** Desplegar la aplicación y realizar pruebas de usuario para asegurar que sea fácil de usar y cumpla con los requisitos de seguridad.

6. Evaluar/Probar la Solución

Para evaluar y probar la solución, podemos seguir estos pasos:

1. **Pruebas de Funcionalidad:** Verificar que la aplicación genera contraseñas correctamente según los criterios especificados.
2. **Pruebas de Seguridad:** Asegurarse de que las contraseñas generadas sean realmente seguras y difíciles de adivinar.
3. **Pruebas de Usabilidad:** Recibir feedback de los usuarios para asegurarse de que la interfaz sea intuitiva y fácil de usar.
4. **Mejoras y Ajustes:** Realizar mejoras basadas en el feedback de las pruebas y asegurarse de que solución esté optimizada.

Diagrama de Caso de Uso

Actores:

1. Usuario

2. Administrador del Sistema

Casos de Uso:

1. Configurar Criterios de Seguridad:

    - El administrador del sistema define los criterios de seguridad para las contraseñas (por ejemplo, longitud mínima, uso de caracteres especiales).

2. Actualizar Base de Datos

    - El administrador actualiza las configuraciones y reglas almacenadas en la base de datos del sistema.

3. Generar Contraseña:

    - El usuario solicita la generación de una contraseña segura.

4. Especificar Longitud:

    - El usuario introduce la longitud deseada para la contraseña.

5. Ver Contraseña Generada:

    - El sistema muestra la contraseña generada al usuario.

6. Guardar Contraseña (Opcional):

    - El usuario puede optar por guardar la contraseña generada en un gestor de contraseñas.

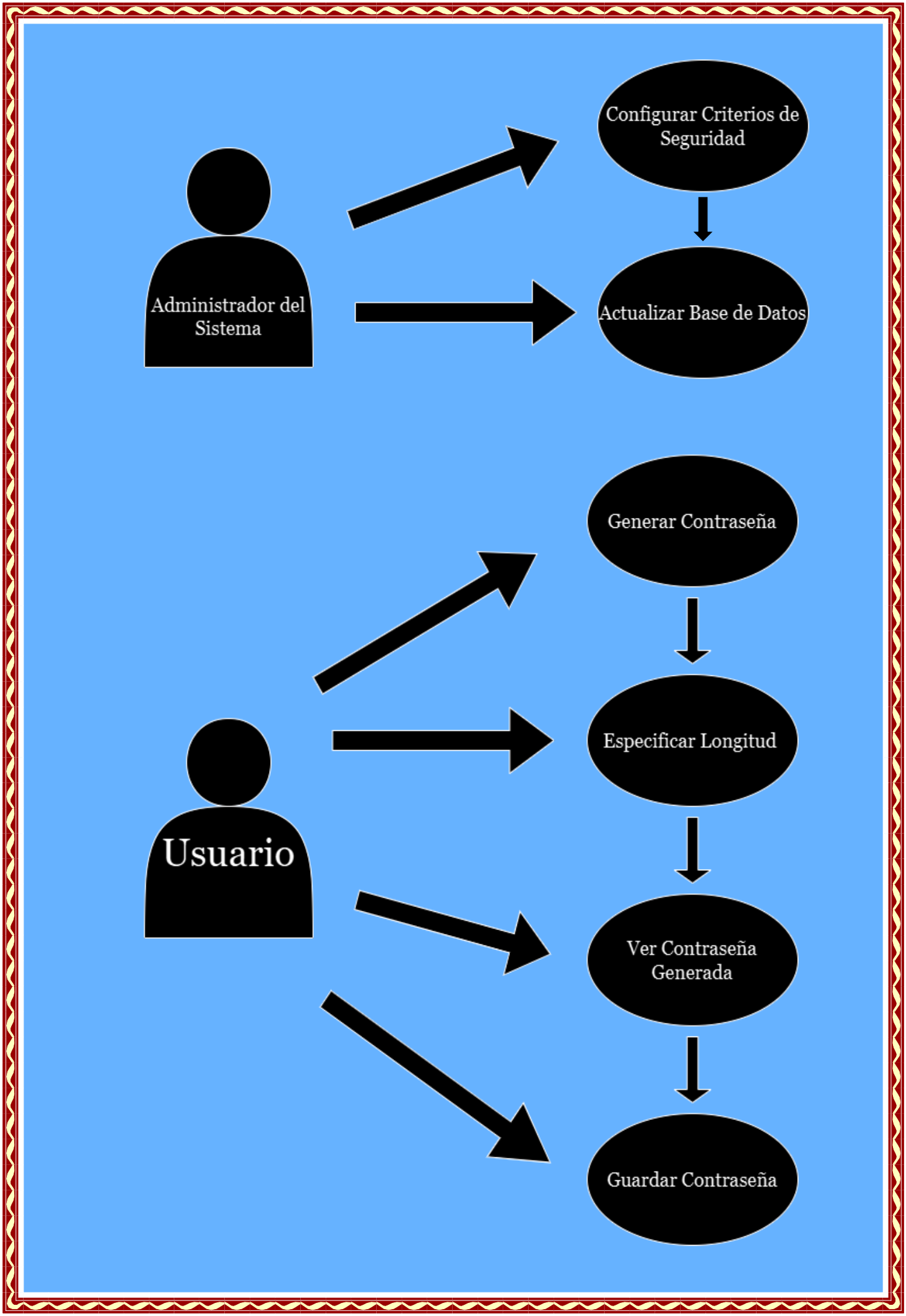
Configurar Criterios de Seguridad
Administrador del Sistema
Actualizar Base de Datos
Generar Contraseña
Especificar Longitud
Usuario
Ver Contraseña Generada
Guardar Contraseña

Diagrama de Componentes

Componentes:

- **Interfaz de Usuario:** Para recibir la entrada del usuario y mostrar la salida.
- **Módulo de Generación de Contraseñas:** Contiene la lógica para generar contraseñas seguras.
- **Módulo de Validación:** Asegura que la contraseña generada cumple con los criterios de seguridad.
- **Base de Datos (opcional):** Para almacenar configuraciones o registros de generación de contraseñas (si se quiere).